Current Specifications

No frozen standard currently exists (although these procedures are quite unlikely to be different from this), however nothing Mobile IP(+) specific has been introduced.

Enhancements

None.

11.6.15 Routing Area Update Accept and Complete

At reception of Insert subscriber data from HLR, the new IGSN will send a Routing Area Update Accept message to the ME. This message will include new RAI, and possibly also new P-TMSI. When the ME has made necessary updates it answers with Routing Area Update Complete.

Current Specifications

No frozen standard currently exists, however nothing Mobile IP(+) specific has been introduced.

Enhancements

None.

Before point a, in figure 11.6a, the connection is established between ME and HA via Source RNC and the old IGSN.

After point b, in figure 11.6a, the connection is established between ME and HA via Target RNC and the new IGSN.

11.7 Traffic Cases

To illustrate how the combined GSM/GPRS/IP System could interwork, some basic traffic cases will be explained in detail below. To give a complete view, also UMTS/GPRS specific procedures have been included, however, not in detail.

11.7.1 Sending Packets

(a) Sending directly to a corresponding host.

(b) Sending via the HA to a corresponding host (use of reverse tunnelling).

11.7.2 Receiving Packets

The following subclause describes how incoming IP datagrams are handled in the different nodes. It is assumed that the Mobile Node has a FA care-of address, which is registered at the HA and that the MN is in (UMTS) idle mode when the incoming datagram arrives. The Mobile IP procedures are according to RFC 2002 [20].

The datagram to the mobile node arrives in the home network via standard IP routing. The HA intercepts the datagram and tunnels it to the care-of address, in this case the FA (IGSN). Before the IGSN can deliver the datagram to the mobile node, paging etc. needs to be performed according to general UMTS/GPRS procedures. This is illustrated in figure 11.7.2a.

If optimised routing is desired and if the correspondent node supports binding cache, the HA sends a binding update message to inform the correspondent node about the current care-of address of the mobile node. From now on, the correspondent node can send datagrams directly to the mobile node by tunnelling them to the FA care-of address.

This is depicted in figure 11.7.2b.

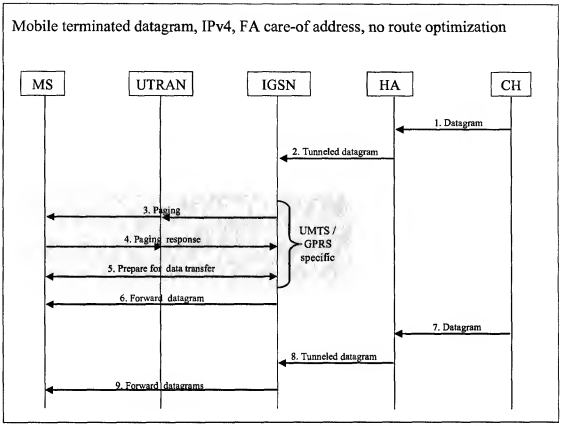

Figure 11.7.2a: Delivery of mobile terminated datagrams, no route optimisation

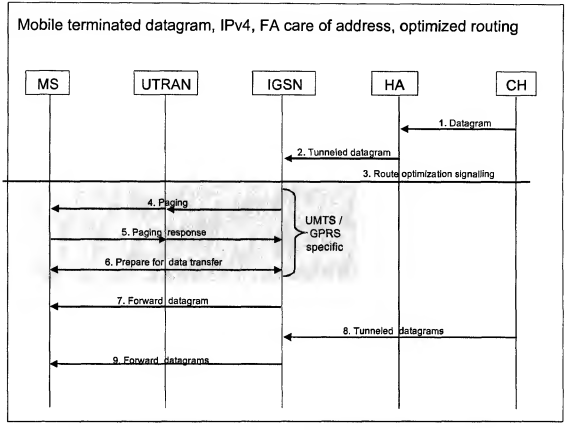

Figure 11.7.2b: Delivery of mobile terminated datagrams, optimised routing

11.8 Service Support

11.8.1 QoS - the Use of Differentiated and Integrated Services

QoS support in UMTS IP CN could be based on either (1) over provisioning of network capacity or (2) IP layer QoS mechanisms. If the IP network, i.e. routers and links, is over provisioned, traffic transported through the network will experience limited packet delays and low packet losses.

In addition, there are currently two IP layer QoS mechanisms under development within IETF, Differentiated Services and Integrated Services.

11.8.1.1 Differentiated Services

The Differentiated Services (DS) architecture [34], [28] is based on a model where IP traffic entering a network is classified and possibly conditioned at the boundaries of the network, and assigned to different behaviour aggregates. Each behaviour aggregate is identified by a single DS code point in the IP header. Within the core of the network, packets are forwarded according to the per-hop behaviour (PHB) associated with the DS code point. This architecture achieves scalability, since per- application flow or per-customer forwarding state not need to be maintained within the core of the network.

There are two per-hop behaviours currently being standardised within IETF, Expedited Forwarding (EF) and Assured Forwarding (AF).

The EF PHB can be used to build a low latency, assured bandwidth, end-to-end service through diffserv domains. To support this service, it is required in every transit node, that the aggregate's maximal arrival rate is less than that aggregate's minimal departure rate. This service appears to the endpoints like a point-to-point connection or a "virtual leased line".

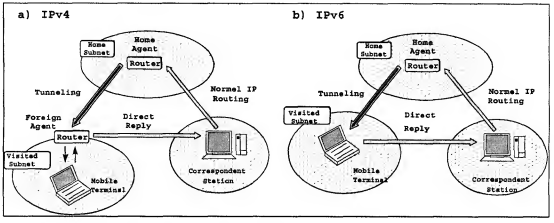

Figure A.1: Basic architecture for supporting IP mobility

A.2 Route optimisation

The operating mode illustrated in the preceding paragraph is extremely simple and enables a mobile terminal to continue to communicate using its own home address even when it is away from its home subnet. The drawback of this consists of the fact that all packets addressed to the mobile terminal must necessarily transit through its home subnet before reaching destination, which makes for:

- an additional load in the home subnet; and
- a longer latency time in transferring traffic to destination.

For this reason, the "mobileip" workgroup is analysing a possible extension (*Route Optimisation*) to the terminal mobility support protocol based on the introduction of a mechanism which enables any station with which an IP level data transfer is in progress (the correspondent node), and not just the home agent, to learn the care-of address associated with the mobile terminal and to use it subsequently to reach the mobile terminal without passing through its home network.

The "mobileip" workgroup is specifying a Route Optimisation protocol for both IPv4 mobility and IPv6 mobility. By contrast with the basic architecture for supporting IP mobility on the Internet, the solutions proposed for IPv6 in this case feature far from negligible differences with respect to those envisaged for IPv4, as the new capabilities supported by the new-generation IP protocol have permitted several architectural options which are not feasible with the current version of the IP protocol.

A.2.1 The solution proposed for IPv4

In the Route Optimisation protocol specified for IPv4, the home agent indicates the mobile terminal's care-of address to the correspondent node when the terminal is away from its home subnet. After receiving a datagram intended for the mobile terminal, the home agent performs a tunnelling operation to the associated care-of address, and also sends an appropriate Binding Update message to the correspondent node. The correspondent node can subsequently send the traffic intended for the mobile terminal directly to its care-of address by means of a tunnelling mechanism, and sets up an optimised route which makes it possible to avoid passing through the home agent (figure A.2).

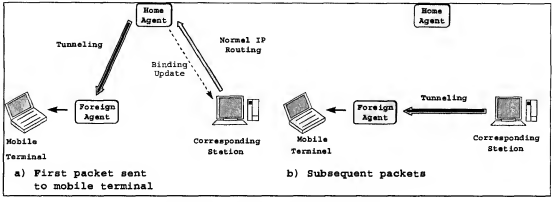

Figure A.2: *Route Optimisation* in IPv4

On its own, however, this procedure is not sufficient to guarantee permanent optimisation of the route to the mobile terminal. A mechanism is also required whereby the correspondent station can learn the mobile terminal's new location every time it moves in the Internet.

Thus, in the IPv4 Route Optimisation protocol, the mobile terminal, after moving in a new subnet, can also communicate its new care-of address to its previous foreign agent. In this way, when a correspondent node attempts to reach the mobile terminal using a care-of address which has become obsolete, the foreign agent which receives transmitted traffic can forward it to the mobile terminal's new location using a tunnelling mechanism. At the same time, the foreign agent sends the home agent a Binding Warning message, asking that the correspondent station be notified of the mobile terminal's new care-of address by means of an appropriate Binding Update message, thus making it possible to restore an optimised route between source and destination (figure A.3).

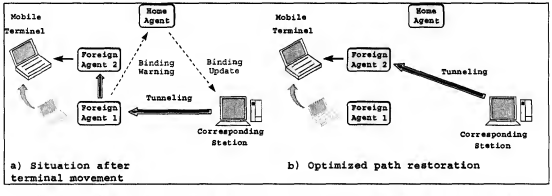

Figure A.3: Mobile terminal movement with notification to the previous foreign agent

If a correspondent node attempts to reach the mobile terminal using an obsolete care-of address and the foreign agent which receives the transmitted traffic does not know the mobile terminal's new location (either because it has not been notified of this location, or because the information has already been removed from its cache), the Route Optimisation protocol suggests that each packet addressed to the mobile terminal be re-routed to the corresponding home agent by means of a tunnel. Once it has reached the home agent, this type of traffic is handled in exactly the same way as any other message addressed to the mobile terminal, and is thus sent to the corresponding care-of address through a new tunnel. At the same time, a Binding Update message is transmitted to the correspondent terminal, once again making it possible to restore a direct path between source and destination (figure A.4).

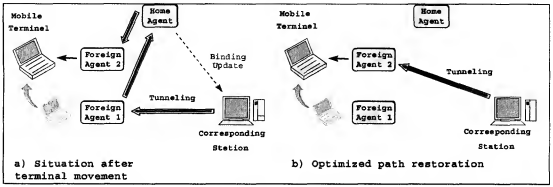

Figure A.4: Mobile terminal movement without notification to the previous foreign agent

The Route Optimisation mechanism specified for IPv4 has the advantage of minimising signalling traffic carried by the portion of the network between the mobile terminal and the foreign agent, as all of the Binding Update messages addressed to the correspondent node are transmitted by the home agent rather than directly by the mobile terminal. This is an extremely important feature, given that the Binding Update messages are coded in UDP packets which are separate from data traffic and thus introduce an overhead that can become unacceptable on a wireless connection such as that between the mobile terminal and the foreign agent.

A.2.2 The solution proposed for IPv6

By contrast with the procedure used in IPv4, the Route Optimisation protocol specified for IPv6 requires that the Binding Update messages intended for the correspondent node be transmitted directly by the mobile terminal every time the latter moves in the Internet (figure A.5). This simplifies the protocol enormously and drastically reduces the latency time before the correspondent node can acquire the mobile terminal's new care-of address.

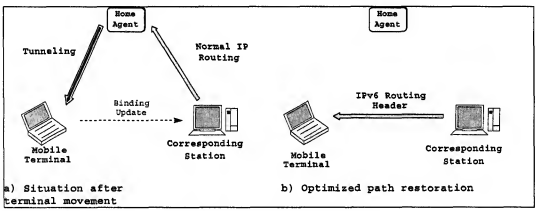

Figure A.5: *Route Optimisation* in IPv6

A solution of this type, which was ruled out in IPv4, becomes feasible with the new-generation IP protocol, given that the Binding Update messages are coded in appropriate IPv6 extension headers[7] and can be included in the same packets which carry effective traffic between the mobile terminal and the correspondent or between the mobile terminal and the home agent. This minimises signalling traffic, making it acceptable to transport it on the network even when the mobile node is connected to the Internet via a wireless interface, which can have a much lower bandwidth than conventional cabled networks and a high error rate.

---

7 In IPv6, the "options" are no longer an integral part of the IP header, as each is memorized in a separate header (called the extension header) located between the IPv6 header and the header of the overlying transport layer (e.g. TCP or UDP). In particular, the options which must be analyzed only by the final destination are specified in a special extension header called the destination options header, which is also used to transport Binding Update messages for IPv6 mobility management.

In addition, while in IPv4 the traffic transmitted by the correspondent node to the mobile terminal is sent directly to its care-of address by means of a tunnelling mechanism, with IPv6 the same result is achieved using a *Routing Header*, i.e. a special extension header that forces the datagram to follow a predetermined route. The advantage of this consists of the fact that the Routing Header introduces a smaller overhead in each packet than would "IPv6 in IPv6" tunnelling, which makes it necessary to introduce a new IPv6 header in each packet transmitted to the mobile terminal.

A.3 Security aspects

Applying IP mobility support protocols in the Internet depends critically on security management.

First of all, the home agent must be able to authenticate messages it receives from the mobile terminal in order to ensure that a false registration cannot cause all of the traffic intended for the mobile terminal to be re-directed to an IP subnet other than that effectively visited.

Moreover, further complications emerge when the Route Optimisation mechanism is used, given that in this case each correspondent node must be able to authenticate the Binding Update messages received from the mobile terminal (IPv6) or from its home agent (IPv4) respectively. In fact, while we can readily accept that the mobile terminal and its home agent, which are normally stations belonging to the same organisation, can be configured manually with a shared secret key used for the authentication algorithms, it is much harder to imagine a similar scenario between the mobile terminal and the correspondent, or between the home agent and the correspondent node, given that the latter may be any Internet station. For this purpose, a mechanism with an appropriate level of security must be developed which enables two stations to agree dynamically on the secret key to be used. A mechanism of this kind has not yet been fully specified by the IETF, though the attention given to this problem by the "ipsec" workgroup is considerable.